Intellectual Property (IP) Protection Policy
# UMC Intellectual Property (IP) Protection Policy

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Letter from Chairman</td>
<td>Page 3</td>
</tr>
<tr>
<td>Document Overview</td>
<td>Page 4</td>
</tr>
<tr>
<td>Production-Related IP Protection</td>
<td>Pages 5-7</td>
</tr>
<tr>
<td>Confidential Document Control</td>
<td>Pages 8-9</td>
</tr>
<tr>
<td>Employee Confidentiality Contract</td>
<td>Pages 10-11</td>
</tr>
<tr>
<td>Employee Education &amp; Training</td>
<td>Page 12</td>
</tr>
<tr>
<td>Audit &amp; Compliance</td>
<td>Page 13</td>
</tr>
</tbody>
</table>
To Our Valued Customers:

In the semiconductor industry, intellectual property (IP) is important and omnipresent, providing the foundation for increasingly complex integrations and implementations on the chip. This presents opportunities as well as challenges to IP developers, semiconductor designers, and foundries. Among the most basic issues is the security of IP – how its integrity and its content can be preserved and protected throughout a complex process that begins from idea to finished product.

This policy document summarizes our formal commitment to IP protection within UMC, outlining how we safeguard your IP and audit compliance. We will gladly respond to any of your questions regarding these polices and are eager to hear suggestions on how they can be improved.

Our commitment to these practices is more than just lip service; rather, it is based on fundamental company beliefs. Our IP policy stems from two principles:

- Partnership - Long-term partnerships provide the greatest success and can exist only in an atmosphere of respect and mutual support.
- Commitment - UMC is committed to the success of our partners; only when that is achieved can we, too, achieve our goals.

To some in the industry, these seem but lofty aspirations. However, we have made these aspirations part of our reality, a reality that will enable our customers to prosper while we also meet our mutual long-term goals for success.

I am confident that you will find these goals reflected in our intellectual property practices. We hope the underlying principles and our detailed procedures demonstrate our commitment to the security of your valuable IP.

Sincerely,

Stan Hung
Chairman
IP Protection Policy-Document Overview

UMC is committed to protecting customer IP throughout the production cycle. Our policy addresses four primary areas, each of which is regularly validated by our internal audit program.

The four primary areas of this policy are:

- Production-related IP Protection
- Confidential Document Control
- Employee Confidentiality Contract
- Employee Training and Education

These four areas are summarized in this document, with flow charts to illustrate the process that UMC executes in order to protect customer IP.

If at any time our customers want more detailed information or would like to personally audit the process, we welcome the inquiry.
I. Production-Related IP Protection

UMC protects its customers' IP in both physical and electronic format throughout the semiconductor manufacturing cycle, including but not limited to: database, WIP status, yield data, masks, and wafers.

- **UMC Production Code Assignment (confidentiality of customer part number)**
  UMC takes considerable precautions to encode customer-specific information and to limit access. Once UMC receives a customer's order, and except when the customer requests otherwise, we generate a "UMC Production Code" to replace the original customer product number. From that point forward, UMC tracks the customer order with the UMC designated number. The original customer product number is kept strictly confidential and is only disclosed to UMC employees on a need-to-know basis.
- **Database Security**

UMC employs high-level security for customer design and database information. The mask tooling group receives a customer’s database in tape form or through electronic transmission to a password-protected database accessible only to the customer and UMC employees with a need-to-know. The database is well protected during and after the mask tooling process. For example, the database is segregated physically and in separate storage from production and other information. Only those employees with specific "need to know" for mask tooling purposes are permitted access. Document control ensures the integrity of our database media storage and management.
- **Mask & Patterned Wafer Management**

UMC safeguards masks and patterned wafers so they are used only for the benefit of the customer for which they are created. Quality assurance personnel enforce the consistency of mask and wafer utilization and disposition. These precautions can be monitored by our customers for their intellectual property through specific records and reports generated for that purpose.
II. Confidential Document Control

UMC has established a stringent process for managing and protecting our customers' confidential documents. Customer confidential documents are separately numbered and tracked, and can be distributed to a UMC employee only on a need-to-know basis. Copies of customer confidential documents are regularly accounted for, and when usage needs have expired, those confidential documents are returned or disposed of according to the UMC document control process.

*Receipt and Management of Incoming Confidential Documents:*

- Non-Disclosure Agreement Signed by UMC and Customer
  - Documents from Customer Received by UMC
    - Documents Transfer List Generated by UMC
      - Approved by Responsible Supervisor
        - Documents Entering into Control by DC
Application and Distribution of Confidential Documents:

Document Control (DC) Managed Documents:

Approved by Application Dept. Manager

Approved by Manager Of Document Owner

Confirmed by DC Manager

Copy, Delivery and Signed For

Disposition of Confidential Documents:

Document control saves the files in the form of .PVF file for authorized colleagues’ online inquiry. Under normal conditions, employees can only read the title. Only with appropriate need-to-know approval, can employees view contents.
III. Employee Confidentiality Contract

To provide further assurance that all UMC employees are fully aware of and sensitive to the critical importance of protecting customer rights, all UMC employees sign a Contract of Employment with specific confidentiality provisions ("confidentiality contract") that affirm their compliance with UMC IP Protection regulations. UMC periodically audits personnel files to verify that all employees have signed our confidentiality contracts and are regularly attending seminars that reinforce the importance of customer rights in confidential information.

Below are relevant confidentiality provisions in UMC's Contract of Employment (translated from Mandarin Chinese).

[Translated extracts]

II. Operational Confidentiality

[...]  
5. During his/her period of employment by UMC and after leaving UMC’s employ, the Employee shall do his/her utmost to prevent any third party from acquiring or becoming aware of any confidential information of UMC including information relating to all equipment and data that either belongs to or should belong to UMC (including reproduction, copies, syntheses, photocopies, handwritten copies, excerpts and translations), as well as all types of valuable knowledge. All information and reports provided by UMC’s chip foundry customers, including but not restricted to design drawings, disks, masks, IC semi-finished products and finished products, as well as all other information that UMC is required to keep confidential, must be kept confidential by the Employee, and must not be disclosed to anyone outside UMC. The Employee shall observe and perform all the terms of any confidentiality or non-disclosure agreement, which UMC is required to observe and perform. In the event of this requirement being violated, the Employee shall indemnify UMC against all liabilities, damages, losses, claims, proceedings, costs and expenses resulting from such violation.
At the time of leaving the company, the Employee will be required to sign a "Declaration of Confidentiality by Personnel Leaving the Company." After his/her resignation, the Employee may not, unless agreed by UMC, use, publicize or disclose to a third party any of the equipment, data, knowledge, news, research and development procedures, research and development results or methods for production process improvement . . . . The Employee understands that in the event of any violation . . . on his/her part, he/she may be liable to legal action being taken against him/her.

- **Re-affirmation and Verification of Confidentiality for Departing Employees**

Upon ending UMC employment, every departing employee is asked to sign a declaration that re-confirms the employee has full knowledge of all the obligations stated in the "Contract of Employment" and that he/she will continue to fulfill those obligations after leaving the company. If deemed necessary, UMC will contact the departed employee's new employer, advising them of the former UMC employee's continuing confidentiality obligations with respect to data, knowledge and information, including but not limited to all the UMC business related materials, acquired while employed at UMC and requesting the new employer help the employee maintain the confidentiality of above-mentioned matters.
IV. Employee Education and Training

UMC provides its employees with mandatory training courses on the subject of protecting IP rights and confidentiality. All employees, from the most junior to the most senior, periodically take refresher courses, which serve as a constant reminder and reinforcement of their obligations with respect to the protection of intellectual property, including our customers' confidential information. Topics for these courses include: IP Importance, Significance, and Laws; IP Protection; Protection of Customer Rights in IP; Protection of Masks, Databases and Wafers; Protection of Confidential Documents and Information; and so forth. Attendance by all employees is tracked and audited regularly. To ensure attentiveness, effectiveness, and an opportunity for employees to have their questions addressed, UMC training courses are conducted by live instructors in a classroom setting, rather than by video or self-study.
V. Audit and Compliance

In order to secure the highest level of quality on a consistent basis, UMC implements a comprehensive "Quality Management Audit" (QMA) program. In this program, representatives from each area of our operations are assigned the specific task of monitoring our quality and compliance. On a regular basis, these teams examine our operations to ensure that each is meeting or exceeding our standards. As part of this QMA, we routinely audit and confirm compliance with our IP Protection Policy.

We welcome customer suggestions and comments on ways to improve our safeguards and, wherever reasonable, act to incorporate these inputs. In short, it is our view that the quality of our services (including the thoroughness of our IP protection) rests upon the dedication of our employees and management, and on our ability to anticipate and respond to customer needs.